UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

KRISTIN TAFOYA, individually and on behalf of all others similarly situated, Plaintiff, v. THOMPSON COBURN, LLP, and PRESBYTERIAN HEALTHCARE SERVICES, Defendants.	Case No. 4:24-cv-1513 JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Kristin Tafoya ("Plaintiff") brings this action on behalf of herself, and all others similarly situated against Defendant, Presbyterian Healthcare Services, ("Presbyterian") and Thompson Coburn LLP ("TC") (collectively "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. Between May 28, 2024, and May 29, 2024, TC, a law firm with "the experience needed to rapidly respond to claims, threatened litigation, and investigations related to data security breaches"[1], lost control over its client Presbyterian Health Care Services' current and former patients' highly sensitive personal information in a data breach perpetuated by cybercriminals ("Data Breach"). On information and belief, the Data Breach affected over 300,000 individuals.[2]

[1] https://www.thompsoncoburn.com/services/practices/cybersecurity/litigation-and-data-breach (last visited November 12, 2024).
[2] https://www.securityweek.com/law-firm-data-breach-impacts-300000-presbyterian-healthcare-

2. Presbyterian chose to allow TC access and control over its current and former patients' highly sensitive personal information.

3. On information and belief, the Data Breach began on or around May 28, 2024, when an unauthorized party gained access to TC's network, and was not discovered by TC until an entire day later, on May 29, 2024, providing cybercriminals unfettered access to Presbyterian's former and current patients' highly private information for two days.

4. Following an internal investigation, TC learned cybercriminals had gained unauthorized access to Presbyterians' patients' personally identifiable information ("PII") and protected health information ("PHI") (collectively "PII/PHI") including but not limited to their names, medical record numbers, patient account numbers, prescription/treatment information, clinical information, and medical provider information.

5. On information and belief, cybercriminals bypassed CL's inadequate security systems to access Presbyterian's current and former patients' PII/PHI in its computer systems.

6. Presbyterian is a New Mexico-based health care system comprised of nine hosptials that serves over 580, 000 members. Upon information and belief, Presbyterian's current and former patients' PII/PHI were involved in the Data Breach.

7. On or about November 6, 2024 –more than five months after the unauthorized party first gained access to patients' PII/PHI– TC and Presbyterian finally notified Class Members about the Data Breach ("Breach Notice") an example of which is attached as **Exhibit A**. However, notification is ongoing, with Plaintiff not receiving her notice until November 6, 2024.

8. Presbyterian's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its patients how many people were impacted, how the breach happened, or

---

patients/ (last visited November 12, 2024).

why it took Defendants more than five months to begin notifying victims that hackers had gained access to highly sensitive PII/PHI.

9. Defendants' failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII/PHI.

10. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII/PHI misuse.

11. In failing to adequately protect Plaintiff's and the Class's PII/PHI, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendants violated state and federal law and harmed an unknown number of its current and former employees.

12. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their PII/PHI. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff Kristin Tafoya is a Data Breach victim.

14. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

PARTIES

15. Plaintiff, Kristin Tafoya, is a natural person and citizen of New Mexico, where she

intends to remain. Plaintiff Tafoya is a Data Breach victim, receiving the Breach Notice on November 6, 2024.

16. Defendant, Presbyterian Healthcare Services, is a New Mexico nonprofit corporation with its principal place of business at 5921 San Mateo Blvd. NE, Albuquerque, NM 87113.

17. Defendant, TC, is a Missouri Corporation, with its principal place of business at One US Bank Plaza, Suite 3500, Saint Louis, MO 63101. Defendant can be served through its registered agent, Roman P. Wuller, at One U.S. Bank Plaza, Suite 2700, St. Louis, MO 63101.

JURISDICTION & VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiff and Defendant TC are citizens of different states.

19. This Court has personal jurisdiction over Defendants because at least one Defendant maintains its principal place of business in this District and does substantial business in this District.

20. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

BACKGROUND FACTS

Thompson Coburn LLP

21. TC is a law firm that touts itself as a "full-service, values-driven law firm with offices strategically located in Birmingham, Chicago, Dallas, Los Angeles, New York, Southern Illinois, St. Louis and Washington, D.C."[3]

22. TC's services are specialized for a "sophisticated client base — including Fortune 500, middle-market and emerging companies — across a range of practice areas and industry sectors"[4] who manage highly sensitive data. Thus, TC must oversee, manage, and protect the PII/PHI of its clients' consumers, including Presbyterian's current and former patients.

23. On information and belief, these third-party patients, whose PII/PHI was collected by TC, do not do any business with TC.

24. In working with third party patients' highly sensitive data, TC assures that it "takes your privacy seriously", boasting that it employs a plethora of ways to ensure the security of PII/PHI:

a. "We use administrative, physical, and technical security measures and safeguards that we consider appropriate to prevent the loss and misuse of data."

b. "We may have written agreements with specific clients related to data security that, as to those specific clients, may provide for additional or different security measures or obligations on our part."[5]

25. TC also claims that its "attorneys have the experience needed to rapidly respond to claims, threatened litigation, and investigations related to data security breaches"[6] and it

[3] https://www.linkedin.com/company/thompson-coburn-llp/about/ (last visited November 12, 2024).
[4] *Id.*
[5] https://www.thompsoncoburn.com/firm/privacy (last visited November 12, 2024).
[6] https://www.thompsoncoburn.com/services/practices/cybersecurity/litigation-and-data-breach (last visited November 12, 2024).

acknowledges that "threats continue to expand and change with increasingly sophisticated attackers (and in some cases, nation states) targeting financial and healthcare systems, industrial control systems and other parts of critical infrastructure."[7]

26. As a self-proclaimed expert in data Privacy and Security and handling highly sensitive aspects of its clients' business, TC understood the need to protect its client's patients' data and prioritize its data security. In fact, TC recognizes that "the consequences of failing to appropriately mitigate cyber vulnerabilities can be devastating."[8]

27. But, on information and belief, TC fails to strictly adhere to these policies in maintaining its client's patients' PII/PHI.

Presbyterian Healthcare Services

28. Presbyterian is a regional hospital system in New Mexico that "provide[s] acute and preventive care: from surgical, ambulatory and emergency services to health fairs, fun runs, and prevention and screening programs."[9] Presbyterian is New Mexico's largest private employer with over 13,000 employees and it boasts a total revenue of over $5.5 billion.[10]

29. In its privacy policy, Presbyterian promises that it has "policies and procedures to protect the privacy of health information that [] identif[ies] you," including:

a. "We have a training program to educate our employees and others about our privacy policies."

[7] https://www.thompsoncoburn.com/services/practices/cybersecurity (last visited November 12, 2024).
[8] *Id.*
[9] https://www.phs.org/about-us (last visited November 12, 2024).
[10] https://www.fiercehealthcare.com/providers/unitypoint-health-presbyterian-healthcare-services-call-11b-merger#:~:text=For%20the%202022%20fiscal%20year,of%20his%20employees%20their%20jobs. (last visited November 12, 2024).

b. "Your health information is only used or shared for our business purposes or as otherwise required or allowed by law."

c. "When a service involving your health information is being performed by a third party, we require a written agreement with them to protect the privacy of your health information."

d. "We are required by law to maintain the privacy of your health information."

e. "We have a legal duty to notify you, and you have a right to know when your protected health information has been inappropriately accessed, used, or disclosed as a result of a breach."

f. "We will not use or share your health information without your written authorization unless required by law."[11]

30. As part of its business, Presbyterian receives and maintains the PII/PHI of thousands of current and former patients. In doing so, Presbyterian implicitly promises to safeguard their PII/PHI.

31. In collecting and maintaining its current and former patients' PII/PHI, Presbyterian agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

32. Despite recognizing its duty to do so, on information and belief, Presbyterian has not implemented reasonably cybersecurity safeguards or policies to protect its patients' PII/PHI or supervised its IT or data security agents and employees, including TC, to prevent, detect, and stop

[11] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://onbaseext.phs.org/PEL/DisplayDocument?ContentID=wcmprod1029971 (last visited November 12, 2024).

breaches of its systems. As a result, Presbyterian left significant vulnerabilities in its storage of Plaintiff's and the Class's PII/PHI for cybercriminals to exploit and gain access to patients' PII/PHI.

The Data Breach

33. Plaintiff is a patient of Presbyterian.

34. As a condition of receiving services from Presbyterian, Defendant requires its patients to disclose PII/PHI including but not limited to, their names, medical records numbers, patient account numbers, prescription/treatment information, clinical information, and medical provider information. Defendant used that PII/PHI to facilitate its business and provision of services to Plaintiff, and required Plaintiff to provide that PII/PHI to obtain services.

35. On information and belief, Presbyterian provided TC with Plaintiff's PII/PHI as part of the legal services TC provided to Presbyterian, including data and privacy advice. Thus, TC was granted access and custody of Plaintiff's PII/PHI including but not limited to name, medical records number, patient account number, prescription/treatment information, clinical information, and medical provider information.

36. On information and belief, Defendants collect and maintain patients' PII/PHI in their computer systems.

37. In collecting and maintaining the PII/PHI, Defendants implicitly agree that they will safeguard the data using reasonable means according to their internal policies and federal law.

38. According to the Breach Notice, TC first detected suspicious activity within its network on May 29, 2024. Following an internal investigation, TC discovered the Data Breach

had occurred between May 28, 2024, and May 29, 2024. Ex. A. In other words, TC's investigation revealed that not only had its network been hacked by cybercriminals at least two days before it discovered the Breach.

39. Despite touting itself to be highly experienced in the Data Privacy and Security sector, TC's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of its clients' patients' highly sensitive PII/PHI. Presbyterian knew or should have known that granting TC access to Plaintiff's PII/PHI would result in a Data Breach given TC's inadequate cybersecurity practices.

40. Additionally, Defendants admitted that PII/PHI was actually stolen during the Data Breach confessing that the information was not just accessed, but that "certain information stored within our environment was viewed **or taken** by an unauthorized actor." Ex. A.

41. On or around November 6, 2024 –over five months after the Breach first occurred– Presbyterian finally began to notify Class Members about the Data Breach.

42. Despite their duties and alleged commitments to safeguard PII/PHI, Defendants do not in fact follow industry standard practices in securing patients' PII/PHI, as evidenced by the Data Breach.

43. In response to the Data Breach, Defendants contend that TC has or will be taking "appropriate measures to promptly address this incident and implemented additional security enhancements." Ex. A. Although Defendants fail to expand on what these alleged "measures" and "enhancements" are, such steps should have been in place before the Data Breach.

44. Through the Breach Notice, Defendants also recognized the actual imminent harm and injury that flowed from the Data Breach, so they encouraged breach victims to "remain

vigilant" "by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors." And, Defendants enclosed a list of "Steps You Can Take to Help Protect Personal Information," including enrolling in credit monitoring services, monitoring accounts, placing fraud alerts on their credit files, placing a credit freeze on their credit reports, and filing a police report if they experience identity fraud. Ex. A.

45. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII/PHI. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

46. On information and belief, Presbyterian has offered only twelve months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Further, the breach exposed patients' nonpublic, highly private information, a disturbing harm in and of itself.

47. Even with complimentary credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII/PHI is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

48. On information and belief, Defendants failed to adequately train and supervise their IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over their patients' PII/PHI. Defendants' negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI.

The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

49. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in similar industries preceding the date of the breach.

50. In light of recent high profile data breaches at other law firm advising and food industry companies[12], Defendants knew or should have known that their electronic records and patients' PII/PHI would be targeted by cybercriminals.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

52. Indeed, cyberattacks against the both the legal and food industry have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII/PHI." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime." [15]

---

[12] *See* https://abovethelaw.com/2023/04/major-biglaw-firm-suffers-cyber-security-breach-of-mergers-acquisitions-data/ (last visited June 23, 2023); https://www.just-food.com/features/tech-leaves-food-industry-more-exposed-to-cybersecurity-threat/ (last visited June 23, 2023); *see also* https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/ (last visited June 23, 2023).

[13] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 23, 2023).

[14] *Id.*

[15] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited June 23, 2023).

53. Cyberattacks on the food industry and legal partner and advisers like Defendants have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly." [16]

54. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including TC and Presbyterian.

Plaintiff Tafoya's Experience

55. Plaintiff Tafoya is a patient of Presbyterian having received services with them for at least ten years.

56. As a condition of receiving services with Presbyterian, Plaintiff was required to provide her PII/PHI, including but not limited to her name, medical records numbers, patient account number, prescription/treatment information, clinical information, and medical provider information.

57. Plaintiff provided her PII/PHI to Presbyterian and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

58. On information and belief, Presbyterian shared Plaintiff's PII/PHI with TC as part of its provision of management legal services and advice to Presbyterian. Presbyterian provided TC with Plaintiff's PII/PHI, including but not limited to her name, medical records number, patient account number, prescription/treatment information, clinical information, and medical provider information.

[16] Secret Service Warn of Targeted, Law360, https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited March 13, 2023).

59. Plaintiff provided her PII/PHI to Defendants and trusted that they would use reasonable measures to protect it according to their internal policies and state and federal law.

60. Defendants deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over five months.

61. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred, researching the Data Breach, and contacting counsel. This time has been lost forever and cannot be recaptured.

62. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII/PHI was exposed in the Data Breach.

63. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

64. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's PII/PHI—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

65. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI being placed in the hands of unauthorized third parties and possibly criminals.

66. Indeed, following the Data Breach, Plaintiff received a notification through Experian that her information had been found on the Dark Web, indicating that her information was in the hands of cybercriminals.

67. Further, shortly after the Data Breach, Plaintiff began experiencing a substantial increase in spam and scam phone calls, suggesting that her PII/PHI has already been placed in the hands of cybercriminals.

68. On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII/PHI that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.

69. Plaintiff has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

70. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII/PHI that can be directly traced to Defendants.

71. As a result of Defendants' failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII/PHI is used;

b. The diminution in value of their PII/PHI;

c. The compromise and continuing publication of their PII/PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII/PHI; and

h. The continued risk to their PII/PHI, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII/PHI in their possession.

72. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

73. The value of Plaintiff's and the Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years, and criminals frequently post stolen PII/PHI openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

74. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

75. One such example of criminals using PII/PHI for profit is the development of "Fullz" packages.

76. Cyber-criminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree

of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

77. The development of "Fullz" packages means that stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

78. Defendants disclosed the PII/PHI of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII/PHI of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

79. Defendants' failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants failed to adhere to FTC guidelines.

80. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PII/PHI.

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PII/PHI that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

82. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

83. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

84. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

85. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

86. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information. [17]

87. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[18]

88. The Data Breach itself resulted from a combination of inadequacies showing Defendants' failure to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[17] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[18] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

89. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

Defendants Failed to Follow Industry Standards

90. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendants. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

91. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

92. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

93. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendants opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

94. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class") defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

> **All individuals residing in the United States whose PII/PHI was compromised in the Data Breach, including all those who received a notice of the Data Breach.**

Excluded from the Class are Defendants, their agents, affiliates, parents, subsidiaries, any entity in which Defendants have a controlling interest, any of Defendants' officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

95. Plaintiff reserves the right to amend the class definition.

96. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the Class, consisting of at least 300,000 members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendants' possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and he has retained counsel

experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

ii. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendants were negligent in maintaining, protecting, and securing PII/PHI;

iv. Whether Defendants breached contract promises to safeguard Plaintiff's and the Class's PII/PHI;

v. Whether Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendants' Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

97. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to

fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(Against Defendants On Behalf of Plaintiff and the Class)

98. Plaintiff realleges all previous paragraphs as if fully set forth below.

99. Plaintiff and members of the Class entrusted their PII/PHI to Defendants. Defendants owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII/PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

100. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII/PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII/PHI —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII/PHI by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

101. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII/PHI. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to

take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

102. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Defendants actively sought and obtained Plaintiff's and the Class's PII/PHI.

103. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendants hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII/PHI —whether by malware or otherwise.

104. PII/PHI is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

105. Defendants breached their duties by failing to exercise reasonable care in supervising their employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII/PHI of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

106. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(Against Defendants On Behalf of Plaintiffs and the Class)

107. Plaintiff realleges all previous paragraphs as if fully set forth below.

108. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII/PHI.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, patients' PII/PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiff's and the members of the Class's PII/PHI.

110. Defendants breached their respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

111. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII/PHI.

112. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII/PHI and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

113. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

114. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

115. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the

healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

116. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect their PHI and by not complying with applicable regulations detailed supra. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

117. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

118. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

119. Had Plaintiff and the Class known that Defendants did not adequately protect their PII/PHI, Plaintiff and members of the Class would not have entrusted Defendants with their PII/PHI.

120. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

121. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of

PII/PHI; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII/PHI, entitling them to damages in an amount to be proven at trial.

122. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants' fails to undertake appropriate and adequate measures to protect their PII/PHI in their continued possession.

COUNT III
Breach of an Implied Contract
(Against Defendant Presbyterian On Behalf of Plaintiff and the Class)

123. Plaintiff realleges all previous paragraphs as if fully set forth below.

124. Plaintiff and Class Members were required to provide their PII/PHI Defendant Presbyterian as a condition of receiving services from Defendant Presbyterian. Plaintiff and Class Members provided their PII/PHI and payment to Defendant in exchange for Defendant's services.

125. Plaintiff and the Class Members accepted Defendant Presbyterian's offers by disclosing their PII/PHI and providing payment to Defendant in exchange for services.

126. Plaintiff and Class Members entered into implied contracts with Defendant Presbyterian under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

127. In providing their PII/PHI, Plaintiff and Class Members entered into an implied contract with Defendant Presbyterian whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII/PHI.

128. In delivering their PII/PHI to Defendant Presbyterian, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

129. Plaintiff and the Class Members would not have entrusted their PII/PHI to Defendant Presbyterian in the absence of such an implied contract.

130. Defendant Presbyterian accepted possession of Plaintiff's and Class Members' PII/PHI.

131. Had Defendant Presbyterian disclosed to Plaintiff and Class Members that Defendants did not have adequate computer systems and security practices to secure patients' PII/PHI, Plaintiff and members of the Class would not have provided their PII/PHI to Defendant.

132. Defendant Presbyterian recognized that patients' PII/PHI is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

133. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant Presbyterian.

134. Defendant Presbyterian breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

135. Defendant Presbyterian breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII/PHI.

136. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by

Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII/PHI; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII/PHI; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendants promised when Plaintiff and the proposed class entrusted Defendants with their PII/PHI; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII/PHI, which remains in the Defendants' possession with inadequate measures to protect Plaintiff's and Class Members' PII/PHI.

Count IV
Breach of Contract
(Against TC On Behalf of Plaintiff and the Class)

137. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

138. Defendant TC entered into various contracts with its clients, including Defendant Presbyterian, to provide legal services to its clients.

139. These contracts are virtually identical to each other and were made expressly for the benefit of Plaintiff and the Class, as it was their confidential information that Defendant TC agreed to collect and protect through its services. Thus, the benefit of collection and protection of the PII/PHI belonging to Plaintiff and the Class were the direct and primary objective of the contracting parties.

140. Defendant TC knew that if it were to breach these contracts with its clients, the clients' consumers, including Plaintiff and the Class, would be harmed by, among other things, fraudulent misuse of their PII/PHI.

141. Defendant TC breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiff's and Class Members' PII/PHI.

142. As reasonably foreseeable result of the breach, Plaintiff and the Class were harmed by Defendant TC's failure to use reasonable data security measures to store their PII/PHI, including but not limited to, the actual harm through the loss of their PII/PHI to cybercriminals.

143. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
Unjust Enrichment
(Against Defendants On Behalf of Plaintiff and the Class)

144. Plaintiff realleges all previous paragraphs as if fully set forth below.

145. This claim is pleaded in the alternative to the breach of implied contractual duty claims.

146. Plaintiff and members of the Class conferred a benefit upon Defendants in providing the PII/PHI to Defendants.

147. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's PII/PHI, as this was used to facilitate the services it sold to Plaintiff and the Class.

148. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff and the Class's PII/PHI because Defendants failed to

adequately protect their PII/PHI. Plaintiff and the proposed Class would not have provided their PII/PHI to Defendants had they known Defendants would not adequately protect their PII/PHI.

149. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT VI
Invasion of Privacy
(Against Defendants On Behalf of Plaintiff and the Class)

150. Plaintiff realleges all previous paragraphs as if fully set forth below.

151. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

152. Defendants owed a duty to Plaintiff and Class Member to keep their PII/PHI confidential.

153. Defendants affirmatively and recklessly disclosed Plaintiff's and Class Members' PII/PHI to unauthorized third-parties.

154. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII/PHI is highly offensive to a reasonable person.

155. Defendants' reckless and negligent failure to protect Plaintiff's and Class Members' PII/PHI constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

156. Defendants' failure to protect Plaintiff's and Class Members' PII/PHI acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

157. Defendants knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

158. Because Defendants failed to properly safeguard Plaintiff's and Class Members' PII/PHI, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

159. As a proximate result of Defendants' acts and omissions, Plaintiff's and the Class Members' private and sensitive PII/PHI was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

160. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendants with their inadequate cybersecurity system and policies.

161. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiff's and the Class's PII/PHI.

162. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII/PHI.

163. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII/PHI;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands that this matter be tried before a jury.

Dated: November 12, 2024 Respectfully submitted,

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com